AMENDMENTS TO THE CLAIMS

Cancel Claims 2 and 12 without prejudice. Please accept amended Claims 1, 11 and 22 as follows:

1. (Currently Amended) A computing device for securely executing authorized code, said computing device comprising:

a protected memory for storing authorized code, which contains an original digital signature, wherein said protected memory is cryptographically protected; and

a processor in signal communication with said protected memory for preparing to execute code from the protected memory by verifying that a digital signature contained in said code is original in accordance with a public key, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution.

2. (Cancelled)

3. (Original) A computing device as recited in claim 1 wherein the integrity of the contents of said protected memory is protected by encryption.

4. (Original) A computing device as recited in claim 1 wherein said protected memory is physically protected.

5. (Original) A computing device as recited in claim 1 wherein said public key is stored in said protected memory.

6. (Original) A computing device as recited in claim 1 wherein at least one of the integrity of said authorized code and the privacy of said authorized code is protected at run time.

7. (Original) A computing device as recited in claim 6 wherein the integrity of said authorized code is protected at run time with symmetric key encryption.

8. (Original) A computing device as recited in claim 6, wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

9. (Original) A computing device as defined in claim 1 wherein:

the protected memory stores code with an original digital signature corresponding to an Owner Public Key; and

the processor verifies the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then verifies the original digital signature in accordance with the Owner Public Key.

10. (Original) A computing device as defined in claim 9, further comprising:

reading means for reading a Certificate containing an Owner Public Key;

validation means for validating the Certificate with the Manufacturer Public Key;

matching means for finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

verification means for using the matched Owner Public Key to verify the authorized code.

11. (Currently Amended) A method for ensuring that a processor will execute only authorized code, said method comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory, wherein said protected memory is cryptographically protected;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code is said protected memory.

12. (Cancelled)

13. (Original) A method as recited in claim 11 wherein the integrity of the contents of said protected memory is protected by encryption.

14. (Original) A method as recited in claim 11 wherein said protected memory is physically protected.

15. (Original) A method as recited in claim 11 wherein said public key is stored in said protected memory.

16. (Original) A method as recited in claim 11 wherein the integrity of said authorized code is protected at run time.

17. (Original) A method as recited in claim 16 wherein the integrity of said authorized code is protected with symmetric key encryption.

18. (Original) A method as recited in claim 11 wherein the privacy of said authorized code is protected at run time.

19. (Original) A method as recited in claim 18 wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

20. (Original) A method as defined in claim 11, further comprising:

storing code in the protected memory with an original digital signature corresponding to an Owner Public Key; and

verifying the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then verifying the original digital signature in accordance with the Owner Public Key.

21. (Original) A method as defined in claim 20, further comprising:

reading a Certificate containing an Owner Public Key;

validating the Certificate with the Manufacturer Public Key;

finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

using the matched Owner Public Key to verify the authorized code.

22. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory, wherein said protected memory is cryptographically protected;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code is said protected memory.